Impact of Cybercrime on Technological and Financial Developments

Suci Ramadani[1], Andysah Putera Utama Siahaan[2], Sutrisno[3], Syafruddin Ritonga[4], Wan Rizca Amelia[5], Hasbiana Dalimunthe[5], Riswan Munthe[6]

[1]Faculty of Social Science, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[3]Faculty of Engineering, Universitas Medan Area, Medan, Indonesia
[4]Faculty of Social and Politic, Universitas Medan Area, Medan, Indonesia
[5]Faculty of Economics and Business, Universitas Medan Area, Medan, Indonesia
[6]Faculty of Law, Universitas Medan Area, Medan, Indonesia

Abstract: *The more sophisticated the technology, the higher the level of criminal activity. Before there was digital data, the world only had physical threats. However, the emergence of the internet and the global network creates cybercrime everywhere. The emergence of this crime is because many companies or organizations are involved in the internet network. For example, purchasing with a credit card requires a manual swipe tool, while now the credit card itself can be transacted online. Cyber attack is one of the crimes that can be experienced by anyone, especially with the increasing number of organizations connected to the Internet to make way for hackers to be able to work on an organization. Large developing markets are not spared from the cybercriminals. The higher their role in the global supply chain increases their attractiveness to attack through cyberspace. Attackers will use it if their site's security management is weak. Cybercrime is too easy to do. Many technology users are failing to perform the most basic protection measures. Many companies only think about their economic circulation without having adequate defense products, while cybercriminals use sophisticated and straightforward technology to identify targets, automate the creation and delivery of software, and easy monetization of what they steal. Cybercrime affects technology and finances a lot in the present. Many individuals, companies or banks suffer huge losses. Cybercrime can be anticipated by increasing security in the corporate network when communicating to the outside world.*

Keywords: *Cybercrime, Law, Technology, Finance.*

1. INTRODUCTION:

Along with the times, the development of information technology can make it easier for people to engage in viewing news and searching for information circulating in cyberspace [1]–[3]. The use of the internet among individuals is inseparable from human life. Various groups, young and mature always enjoy this facilitation. Technology advances give a negative and positive influence on technology today [4]. Starting from any news that we might be able to see on social media there is much information circulating which is useful for us to be able to maximize all the activities that exist today. Using technology, all activities can run quickly and practically so that it helps a lot for our future activities. The positive impact of technological developments in today's circles can facilitate finding information and facilitate work depending on how technology can benefit business and others [5]–[7] The negative impact of technological development is the emergence of cybercrime everywhere [8]–[10]. This crime is carried out without having to do physical activities. Only by sitting in front of a computer can this crime be committed and negatively impact the company's morning. The company that is most disadvantaged when cybercrime occurs is the bank. Banks are financial sources. It has always been the target of criminals. At banks, there are many customer accounts targeted by cybercrime [11]. The use of technology is used for irresponsible matters. Internet network technology can facilitate cybercrime actions to occur. World finance can suffer huge losses. Many stocks fall when a company is hacked and harmed by cybercrime. The development of technology can plunge business actors towards the negative [12].

2. THEORIES:

Cybercrime is not a crime committed by a wild party by using computer technology as a significant crime tool. It works with global network mediation. It cannot work if a system is not connected to a global network. It is a crime that utilizes the development of internet technology. It is defined as an unlawful act that utilizes computer technology based on the sophistication of the development of internet technology [13]. The types and violations of cybercrime are very diverse. It happens because the development and application of technology support it [14]. Cybercrime can be in the form of wiretapping and misuse of electronic or electronically transferred information or data, electronic data theft, pornography, child abuse as objects against the law, internet fraud, internet gambling, website destruction, in addition to system destruction through viruses, Trojan Horse, grounding signal and others [15]. The perpetrators of cybercrime

come from people who are experts in networking. Usually, cybercrimes are more than one person. For high-class crimes, cybercrime has a particular team. Cybercrime principals generally master algorithms and computer programming for creating viruses or malware [16]. The perpetrator can read how the system, network, and find the system slot. The weakness is used to be able to enter so that criminal acts such as data theft can be successfully carried out [17]–[19]. There are several types of crime in cybercrime that can be classified according to activity, such as:

- Unauthorized Access
- Illegal Contents
- Deliberate virus spread
- Cyber Espionage, Sabotage, and Extortion
- Carding
- Hacking and Cracker
- Cybersquatting and Typosquatting
- Cyber Terrorism

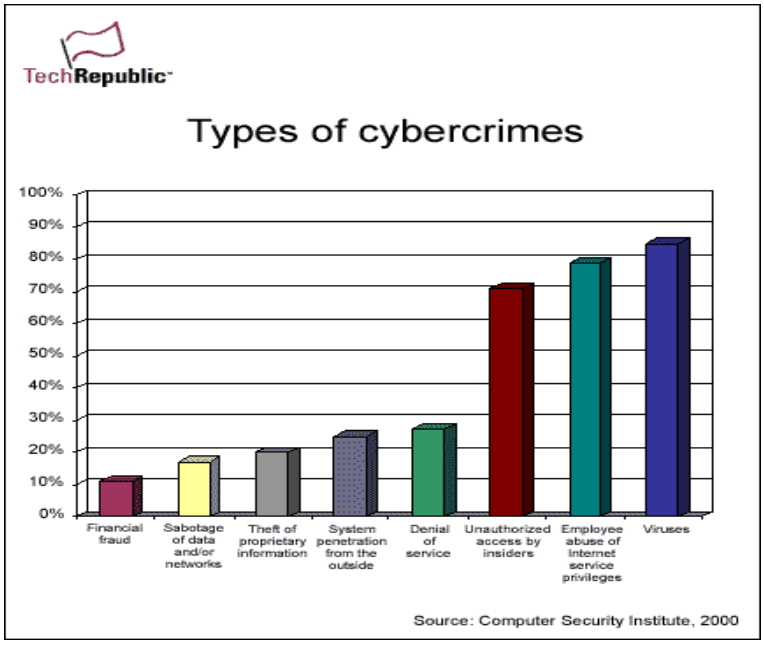

Figure 1. Types of Cybercrimes

Figure 1 describes the measurement of cybercrime based on type taken from TechRepublic in 2000. The most significant type is viruses while financial fraud is the smallest number. There are eight types of cybercrime which are sorted from small to large. From 1998 to 2000, there has been a $129 million increase in estimated reported losses due to cybercrime. It's easy to understand why sales of security software and hardware have also jumped, as shown in the following figure [20].

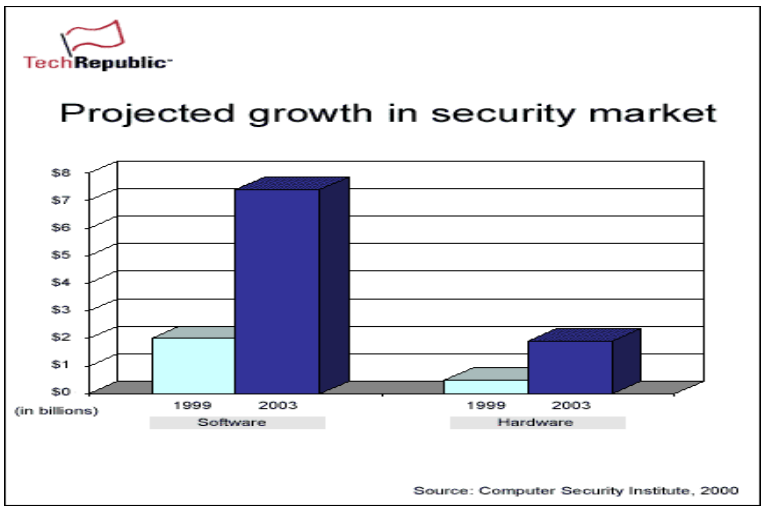

Figure 2. Projected growth in security market

3. RESULT AND DISCUSSION:

Rapid technological developments affect the security of computer network systems. System security has become a necessity for all electronic system providers, both government and business institutions. Unfortunately, there are still many institutions that underestimate ICT security. Information security is not merely a technical aspect, or merely a fulfillment of policy and procedure documents. However, it is a management cycle starting from planning, implementing, evaluating, and improving efforts. Banking and financial industries that use online transactions are required to have a good and reliable security system. Internet Service Providers must have filters in selecting content that contains dangerous information.

3.1 Impact of Cybercrime

Technological developments appear in a row. The trend shows that internet technology is used to help work and conduct business activities. This activity includes students, students, employees, and the upper classes. Cyber technology is a system that is implemented to facilitate fast and instant relationships. If the system does not have a defense, then this will be a threat and target from wild parties. The use of information technology is to provide benefits to the community also has the opportunity to be misused to commit crime both ordinary and professional which has an impact on massive financial losses. Negative impacts can lead to the collapse of the social order system, the paralysis of the country's economy, the weakness of the defense system and can also be used for terror devices.

Cybercrime is a crime that is most detrimental to state finances. Each country has established several laws to regulate the law of cybercrime. Education in information technology and national defense has been included in the curriculum in universities. It will explain the impact caused by cybercrime. Introduction Various types of information technology in digital form are popular, and in demand by the world community, the internet is one of them. With the internet, there are various kinds of applications that can be used by computer users such as to communicate, find news and do business. Software development triggers cybercrime. Initially, the software used to commit crimes is software for system repair. In repairing the system, software must look for errors in the system. This software is converted to look for weaknesses in the system to be hacked so that when the system experiences weakness, this tool will work well. The development of information and communication technology certainly adds to the trend of world technological development with all forms of human creativity. The development of technology extends to various fields where people can quickly obtain the information anytime.

Companies in doing business depend a lot on banks because they have an online transaction system. Without realizing it, online transactions can cause enormous losses for the business person. The mistake that often occurs is neglect of maintaining privacy and account. Business can also be done anywhere as long as there is internet access. Even important information is stored on a computer and can be accessed anywhere because the data is stored online. It is also what causes cybercrime. The bank also runs the banking process using internet access. For example, ATM has its network that can be accessed by customers anywhere. If cybercrime perpetrators can enter the ATM system, funds owned by customers will be lost one by one. The use of computers will also be disrupted so that the banking process cannot run smoothly. Information related to customer data can be misused.

3.2 Cybercrime Eradication

Cybercrime can be eradicated by developing doctrines and strategies that involve all parties who understand information and communication to form a draft and basic concept as a guide. If a country can provide support to the parties involved, cybercrime can be slowly eradicated or reduced. To be able to develop everything that is needed in the face of a threat, the security of attacks from advances in technology and information, especially on global cyber development, the fundamental is the resources and the ability to create software and hardware, to unite the components of strength and can create a devices that can work well.

Crime activities with computers or computer networks can be anticipated by learning more about the impact and origin of cybercrime. Cybercrime perpetrators can make many patterns and many ways also prevent the occurrence of cybercrime. To protect and prevent unwanted losses in business can be done by gaining the security system. Another way in which a company can prevent cybercrime or hackers from attacking businesses and banks is by having an IT security officer to maintain and maintain the systems that the company has. These security specialists can conduct security checks and make notifications to the company whether the security system needs to be improved or not. IT consultants can make recommendations about how the system in the company can be improved. More and more cybercrime perpetrators are continually looking for loopholes to enter and gain access to company data and steal valuable information with different goals. Companies that can hire IT security consultants and people who know how to eradicate cybercrime and use its ability to help and supervise banks in companies. It is also to help improve the company's security infrastructure.

4. CONCLUSION:

Cybercrime is an illegal act. It is detrimental to the rights of computer network users and business people. The presence of cybercrime harms many parties. Every country must have strict rules for cybercrime perpetrators. But not

all cybercrime can be detected. The law that is made must have a guideline that varies. However, the law cannot adequately regulate internet users. The internet is a free network, so it is difficult to detect and prove cybercrime. The state must be able to establish cooperation with the system providers to re-examine the level of security available to the company. By implementing some of these things, in the future cybercrime can be dealt with early. Laws cannot be fully implemented; there is a need for support from all parties so that the law can work by the objectives and the awareness of each party to use technology appropriately.

REFERENCES:

1. Andre Hasudungan Lubis, S. Z. S. Idrus, and A. Sarji, "ICT Usage Amongst Lecturers and Its Impact Towards Learning Process Quality," *Malaysian J. Commun.*, vol. 34, no. 1, pp. 284–299, 2018.
2. D. Kurnia, H. Dafitri, and A. P. U. Siahaan, "RSA 32-bit Implementation Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 279–284, 2017.
3. I. J. Tarigan, B. Alamsyah, S. Aryza, A. P. U. Siahaan, and M. I. Indrawan, "Crime Aspect of Telemedicine on Health Technology," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 10, pp. 480–490, 2018.
4. V. Homburg, "ICT, E-Government and E-Governance: Bits & Bytes for Public Administration," in *The Palgrave Handbook of Public Administration and Management in Europe*, Springer, 2018, pp. 347–361.
5. H. A. Dawood, "Graph Theory and Cyber Security," in *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, 2014, pp. 90–96.
6. H. A. Hasibuan, R. B. Purba, and A. P. U. Siahaan, "Productivity Assessment (Performance, Motivation, and Job Training) using Profile Matching," *Int. J. Econ. Manag. Stud.*, vol. 3, no. 6, pp. 73–77, 2016.
7. N. Kshetri, "The simple economics of cybercrimes," *IEEE Secur. Priv. Mag.*, vol. 4, no. 1, pp. 33–39, Jan. 2006.
8. S. Ramadhani, Y. M. Saragih, R. Rahim, and A. P. U. Siahaan, "Post-Genesis Digital Forensics Investigation," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 164–166, 2017.
9. S. Haryati, A. Ikhwan, D. Arisandi, Fadlina, and A. P. U. Siahaan, "Quality Assurance in Knowledge Data Warehouse," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, p. 239–242], 2017.
10. A. Lubis and A. P. U. Siahaan, "Network Forensic Application in General Cases," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 41–44, 2016.
11. M. Dion, "Corruption, fraud and cybercrime as dehumanizing phenomena," *Int. J. Soc. Econ.*, vol. 38, no. 5, pp. 466–476, Apr. 2011.
12. V. C. E. Tarigan, L. R. Hasibuan, R. B. Purba, Irawan, P. B. Sari, Y. Rossanty, and M. D. T. P. Nasution, "CYBERCRIME CASE ON SOCIAL MEDIA IN INDONESIA," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 7, pp. 783–788, 2018.
13. X. Fu, Z. Ling, W. Yu, and J. Luo, "Cyber Crime Scene Investigations (C^2SI) through Cloud Computing," in *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, 2010, pp. 26–31.
14. C. Novan and M. N. N. Sitokdana, "Pengaruh Cybercrime di Indonesia," *KOMAPO*, 2013. [Online]. Available: http://komapo.org/index.php/teknologi/49-teknologi/112-pengaruh-cybercrime-di-indonesia.html.
15. Y. M. Saragih and A. P. U. Siahaan, "Cyber Crime Prevention Strategy in Indonesia," *SSRG Int. J. Humanit. Soc. Sci.*, vol. 3, no. 6, pp. 22–26, 2016.
16. M. Saragih, H. Aspan, and A. P. U. Siahaan, "Violations of Cybercrime and the Strength of Jurisdiction in Indonesia," *Int. J. Humanit. Soc. Stud.*, vol. 5, no. 12, pp. 209–214, 2017.
17. M. D. T. P. Nasution, Y. Rossanty, A. P. U. Siahaan, and S. Aryza, "The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 6, pp. 1583–1592, 2018.
18. D. J. Neufeld, "Understanding Cybercrime," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–10.
19. Haryanto, A. P. U. Siahaan, R. Rahim, and Mesran, "Internet Protocol Security as the Network Cryptography System," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 223–226, 2017.
20. M. Johnston, "Cybercrime is on the rise," *TechRepublic*, 2000. [Online]. Available: https://www.techrepublic.com/article/cybercrime-is-on-the-rise/. [Accessed: 20-Oct-2018].